MAIL STOP APPEAL BRIEF-PATENTS
8008-1048

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Mao MASUHIRO et al. Appeal No. _____

Serial No. 10/728,820 Group 2146

Filed December 8, 2003 Examiner S. Sciacca

MAINTENANCE INTERFACE USER AUTHENTICATION METHOD AND APPARATUS IN CLIENT/SERVER TYPE DISTRIBUTION SYSTEM

APPEAL BRIEF

MAY IT PLEASE YOUR HONORS: December 9, 2008

1. Real Party in Interest

The real party in interest in this appeal is the current assignee, NEC Corporation of Tokyo, Japan.

2. Related Appeals and Interferences

None.

3. Status of Claims

Claims 1-32, 37-44, and 49-56 were rejected and are the subject of the present appeal. Claims 33-36 and 45-48 have been canceled.

4. Status of Amendments

No amendments were filed following the final rejection of April 11, 2008.

5. Summary of Claimed Subject Matter

Claims 1, 17, 37, and 49 are independent. The dependent claims are not argued separately.

The present invention relates to a maintenance interface user authentication method and apparatus in a client/server type distribution system. The method and apparatus find use when maintenance is to be performed on a computer device that uses authentication for accessing the computer device. The maintenance interface user authentication method and apparatus can set and nullify user authentication information for authentication of a user at the time of using a maintenance interface provided in a client device from a server device over a network (page 1, lines 6-14).

Claim 1 defines a maintenance interface user authentication apparatus in a client/server type distribution system having a plurality of client devices (Figure 1, element 3) connected to a server device (Figure 1, element 1) over a network (Figure 1, element 6; page 30, lines 4-8).

The server device includes a request receiving section (Figure 1, element 11; page 31, lines 9-13) which receives from a server-side console (a) a user authentication information setting request including user authentication information and designation of the client devices and (b) a nullification-of-user-authentication-information-setting request including designation of the client devices (Figure 2, step S101 and Figure 3 step S111). The server device also includes a request transfer section (Figure 1, element 12; page 31, lines 14-16; page 32, lines 7-16; page 33, lines 8-14) which transfers (a) the user authentication information setting request and (b) the nullification-of-user-authentication-information-setting request, received by the request receiving section, to those of the client devices which are designated over the network (Figure 2, step S105 and Figure 3, step S114).

Each of the client devices has a user authentication section (Figure 1, element 32) which authenticates a user at a time of using a maintenance interface based solely on the user authentication information from the server device and without regard for prior authentication information in the client devices (Figure 4, step 122; page 34, lines 1-3, lines 18-22; page 35, line 9 through page 36, line 15; Figure 10 and the related discussions at page 39, line 10 through page 41, line 17

and page 43, line 24 through page 45, line 11). Each client device also includes a remote request processing section (Figure 1, element 33) which sets the user authentication information, included in the user authentication information setting request, in the user authentication section when receiving the user authentication information setting request from the server device over the network, and nullifies the user authentication information set in the user authentication section when receiving the nullification-of-user-authentication-information-setting request from the server device over the network (page 34, lines 3-8; page 35 lines 4-12 and 17-24; Figure 4, step S124 and Figure 5, step S133).

Independent claim 17 defines a method that generally corresponds to the system defined in claim 1. The method includes (a) a step in which the server device receives a user authentication information setting request including user authentication information and designation of client devices from a server-side console and transfers the user authentication information setting request to the designated client devices over a network (Figure 2, steps S101 and S105; page 31, lines 9-16). The method further includes (b) a step in which the client devices receive the user authentication information setting request over the network and set the user authentication

information setting request in a user authentication section which authenticates a user at a time of using a maintenance interface based solely on the user authentication information from the server device and without regard for prior authentication information in the client devices (Figure 4, steps S121 and S124; page 34, lines 3-8).

With regard to nullification, the method of claim 17 includes (c) a step in which the server device receives a nullification-of-user-authentication-information-setting request including designation of the client devices from the server-side console and transfers the nullification-of-user-authentication-information-setting request to the designated client devices over the network (Figure 3, steps S111 and S114; page 33, lines 8-14). The method further includes (d) a step in which the client devices receive the nullification-of-user-authentication-information-setting request over the network and nullify the user authentication information set in the user authentication section (Figure 5, steps S131 and S133; page 35, lines 4-12 and 17-24).

Claim 37 defines a client device that generally corresponds to the client devices in claims 1 and 17. The client device has a user authentication section (Figure 1, element 32) which authenticates a user at a time of using a maintenance interface

based solely on the user authentication information from the server device and without regard for prior authentication information in the client devices (Figure 4, step 122; page 34, lines 1-3, lines 18-22; page 35, line 9 through page 36, line 15; Figure 10 and the related discussions at page 39, line 10 through page 41, line 17 and page 43, line 24 through page 45, line 11). The client device also includes a remote request processing section (Figure 1, element 33) which sets the user authentication information, included in the user authentication information setting request, in the user authentication section when receiving the user authentication information setting request from the server device over the network, and nullifies the user authentication information set in the user authentication section when receiving the nullification-of-user-authentication-information-setting request from the server device over the network (page 34, lines 3-8; page 35 lines 4-12 and 17-24; Figure 4, step S124 and Figure 5, step S133).

Claim 49 defines a computer readable medium with a program stored therein that causes a computer constituting a client device to function as the client device in claim 37. That is, the client device has a user authentication section (Figure 1, element 32) which authenticates a user at a time of using a maintenance interface based solely on the user authentication

information from the server device and without regard for prior authentication information in the client devices (Figure 4, step 122; page 34, lines 1-3, lines 18-22; page 35, line 9 through page 36, line 15; Figure 10 and the related discussions at page 39, line 10 through page 41, line 17 and page 43, line 24 through page 45, line 11). The client device also includes a remote request processing section (Figure 1, element 33) which sets the user authentication information, included in the user authentication information setting request, in the user authentication section when receiving the user authentication information setting request from the server device over the network, and nullifies the user authentication information set in the user authentication section when receiving the nullification-of-user-authentication-information-setting request from the server device over the network (page 34, lines 3-8; page 35 lines 4-12 and 17-24; Figure 4, step S124 and Figure 5, step S133).

6. Grounds of Rejection to be Reviewed on Appeal

Whether claims 1-32, 37-44, 49-56 are unpatentable under 35 U.S.C. 103(a) over GB 2 360 107 (hereinafter GB '107) in view of O'DONNELL et al.

7. Argument

Rejection of claims 1-32, 37-44, 49-56 under 35 U.S.C. 103(a) over GB'107 and O'DONNELL et al.

Claims 1, 17, 37, and 49

These claims provide, among other features, that authentication is based solely on the user authentication information from the server device and without regard for prior authentication information in the client device. As explained below, the references do not disclose or suggest that authentication when opening a maintenance interface in the client device is to be based solely on the input from the server without regard for prior authentication information. In the prior art, the authentication is predicated on permission from a client device, not based solely on the user authentication information from the server (e.g., GB'107 Figure 13, element 1310 and page 21, lines 9-21; and O'DONNELL et al. column 8, lines 15-62).

GB'107 describes a framework by which security policy and application guards are distributed from a policy manager located in a server. The reference does not disclose that permission to open a maintenance interface at a client device can be carried out from a maintenance console of a server. In GB'107 a series of actions are commenced by a permission request from a client

device. By contrast, in the present invention, actuation of a maintenance console at a client device is enabled by permission given from the maintenance console of a server regardless of the permission request from the client device.

O'DONNELL et al. describe a system in which a client device (user) is able to dynamically grant or deny permission for a technical support representative to access the user's data. That is, authorization depends on access granted by the user, not solely on user authentication information from the server. Note, for example, that in column 8 O'DONNELL et al. refer to the user specifying data to which the support representative is authorized to access. The support representative is authorized access to the client device and cannot connect to the client device without access from the client-side console. There is nothing in the reference that suggests that authentication is to be based solely on the user authentication information from the server device and without regard for prior authentication information in the client device. Indeed, O'DONNELL et al. predicate authorization on actions by the client device (e.g., column 8, lines 49-53).

The Examiner refers to column 4, lines 65-67, column 5, line 1, and Figure 3 of O'DONNELL et al. However, this is an overview and the details at column 8 explain what is meant by

the Examiner's citation. As noted above, authorization depends at least in part on actions by the client device, and is thus not based solely on the user authentication information from the server device and without regard for prior authentication information in the client device.

Accordingly, there is no suggestion in the combination that authentication is based solely on the user authentication information from the server device and without regard for prior authentication information in the client device, and thus the claims avoid the rejection under §103.

The dependent claims are allowable by reason of their dependence on one the above independent claims.

In view of this, it is believed that the rejection of record cannot be sustained and that the same must be reversed and such is respectfully requested.

The claims involved in the appeal are set forth in the Claims Appendix.

There are no copies of evidence in the Evidence Appendix.

There are no copies of decisions in the Related Proceedings Appendix.

Respectfully submitted,

YOUNG & THOMPSON

By ___/Thomas W. Perkins/_____
Thomas W. Perkins
Attorney for Appellants
Registration No. 33,027
209 Madison Street, Suite 500
Alexandria, VA 22314
Telephone: 703/521-2297

TWP/lk

8. Claims Appendix

The claims on appeal:

1. A maintenance interface user authentication apparatus in a client/server type distribution system having a plurality of client devices connected to a server device over a network,

said server device having:

a request receiving section which receives from a server-side console a user authentication information setting request including user authentication information and designation of said client devices and a nullification-of-user-authentication-information-setting request including designation of said client devices; and

a request transfer section which transfers said user authentication information setting request and said nullification-of-user-authentication-information-setting request, received by said request receiving section, to those of said client devices which are designated over said network,

each of said client devices having:

a user authentication section which authenticates a user at a time of using a maintenance interface based solely on said user authentication information from said server device and without regard for prior authentication information in said client devices; and

a remote request processing section which sets said user authentication information, included in said user authentication information setting request, in said user authentication section when receiving said user authentication information setting request from said server device over said network, and nullifies said user authentication information set in said user authentication section when receiving said nullification-of-user-authentication-information-setting request from said server device over said network.

2. The maintenance interface user authentication apparatus according to claim 1, wherein setting of said user authentication information in said user authentication section in each of said client devices can be done only from said server-side console.

3. The maintenance interface user authentication apparatus according to claim 1, wherein said server device has an encryption section which encrypts said user authentication information in said user authentication information setting request to be transferred by said request transfer section, and each of said client devices has a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received by said remote request processing section.

4. The maintenance interface user authentication apparatus according to claim 1, wherein each of said client devices has a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again by a new user authentication information setting request received over said network.

5. The maintenance interface user authentication apparatus according to claim 1, wherein each of said client devices has a use time management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section.

6. The maintenance interface user authentication apparatus according to claim 5, wherein each of said client devices has a use time extending section which extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface.

7. The maintenance interface user authentication apparatus according to claim 6, wherein at a time a first log-in request is issued since opening of said maintenance interface, said use time extending section determines whether or not a remaining use time managed by said use time management section lies within a predetermined given time and extends said remaining use time of said use time management section by a predetermined extension time when said remaining use time lies within said predetermined given time.

8. The maintenance interface user authentication apparatus according to claim 6, wherein during first log-in since opening of said maintenance interface, said use time extending section determines whether or not a remaining use time managed by said use time management section has fallen within a predetermined given time and extends said remaining use time of said use time management section by a predetermined extension time when said remaining use time has fallen within said predetermined given time.

9. The maintenance interface user authentication apparatus according to claim 5, wherein said use time management section uses, as said allowable use time, an allowable use time designated in said user authentication information setting request sent from said server device.

10. The maintenance interface user authentication apparatus according to claim 5, wherein said use time management section uses an allowable use time reference value prestored in said client devices as said allowable use time.

11. The maintenance interface user authentication apparatus according to claim 5, wherein when an allowable use time is designated in said user authentication information setting request sent from said server device, said use time management section uses said designated allowable use time as said allowable use time, and when said allowable use time is not designated, said use time management section uses an allowable use time reference value prestored in said client devices as said allowable use time.

12. The maintenance interface user authentication apparatus according to claim 1, wherein each of said client devices has a log-in number management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section.

13. The maintenance interface user authentication apparatus according to claim 12, wherein said log-in number management

section uses, as said allowable number of log-in events, an allowable number of log-in events designated in said user authentication information setting request sent from said server device.

14. The maintenance interface user authentication apparatus according to claim 13, wherein said log-in number management section uses an allowable-number-of-log-in reference value prestored in said client devices as said allowable number of log-in events.

15. The maintenance interface user authentication apparatus according to claim 13, wherein when an allowable number of log-in events is designated in said user authentication information setting request sent from said server device, said log-in number management section uses said designated allowable number of log-in events as said allowable number of log-in events, and when said allowable number of log-in events is not designated, said log-in number management section uses an allowable-number-of-log-in reference value prestored in said client devices as said allowable number of log-in events.

16. The maintenance interface user authentication apparatus according to claim 1, wherein each of said client devices has an authentication nullification section which nullifies said user authentication information set in said user authentication

section at a time a user of said maintenance interface ends use of said maintenance interface.

17. A maintenance interface user authentication method in a client/server type distribution system comprising:

(a) a step in which a server device receives a user authentication information setting request including user authentication information and designation of client devices from a server-side console and transfers said user authentication information setting request to said designated client devices over a network;

(b) a step in which said client devices receive said user authentication information setting request over said network and set said user authentication information setting request in a user authentication section which authenticates a user at a time of using a maintenance interface based solely on said user authentication information from said server device and without regard for prior authentication information in said client devices;

(c) a step in which said server device receives a nullification-of-user-authentication-information-setting request including designation of said client devices from said server-side console and transfers said nullification-of-user-authentication-information-setting request to said designated

client devices over said network; and

(d) a step in which said client devices receive said nullification-of-user-authentication-information-setting request over said network and nullify said user authentication information set in said user authentication section.

18. The maintenance interface user authentication method according to claim 17, wherein setting of said user authentication information in said user authentication section in each of said client devices can be done only from said server-side console.

19. The maintenance interface user authentication method according to claim 17, wherein said step (a) includes a process of causing said server device to encrypt said user authentication information to be transferred and said step (b) includes a process of causing said client devices to decrypt said received user authentication information.

20. The maintenance interface user authentication method according to claim 17, wherein said step (b) includes a process of forcibly disabling use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again to new user authentication information received.

21. The maintenance interface user authentication method according to claim 17, further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section.

22. The maintenance interface user authentication method according to claim 21, further including:

(f) a step in which said each of said client devices extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface.

23. The maintenance interface user authentication method according to claim 22, wherein at a time a first log-in request is issued since opening of said maintenance interface, said step (f) determines whether or not a remaining use time managed in said step (e) lies within a predetermined given time and extends said remaining use time by a predetermined extension time when said remaining use time lies within said predetermined given time.

24. The maintenance interface user authentication method according to claim 22, wherein during first log-in since opening of said maintenance interface, said step (f) determines whether or not a remaining use time managed in said step (e) has fallen within a predetermined given time and extends said remaining use time by a predetermined extension time when said remaining use time has fallen within said predetermined given time.

25. The maintenance interface user authentication method according to claim 21, wherein as said allowable use time in said step (e), an allowable use time designated in said user authentication information setting request sent from said server device is used.

26. The maintenance interface user authentication method according to claim 21, wherein as said allowable use time in said step (e), an allowable use time reference value prestored in said client devices is used.

27. The maintenance interface user authentication method according to claim 21, wherein when an allowable use time is designated in said user authentication information setting request sent from said server device, said designated allowable use time is used as said allowable use time in said step (e), and when said allowable use time is not designated, an allowable use time reference value prestored in said client devices is

used as said allowable use time.

28. The maintenance interface user authentication method according to claim 17, further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section.

29. The maintenance interface user authentication method according to claim 28, wherein as said allowable number of log-in events in said step (e), an allowable number of log-in events designated in said user authentication information setting request sent from said server device is used.

30. The maintenance interface user authentication method according to claim 29, wherein as said allowable number of log-in events in said step (e), an allowable-number-of-log-in reference value prestored in said client devices is used.

31. The maintenance interface user authentication method according to claim 29, wherein when an allowable number of log-in events is designated in said user authentication information setting request sent from said server device, said designated

allowable number of log-in events is used as said allowable number of log-in events in said step (e), and when said allowable number of log-in events is not designated, an allowable-number-of-log-in reference value prestored in said client devices is used as said allowable number of log-in events.

32. The maintenance interface user authentication method according to claim 17, further including:

(e) a step in which each of said client devices nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface.

33-36. (canceled)

37. A client device to be connected to a server device over a network, comprising:

a user authentication section which authenticates a user at a time of using a maintenance interface based solely on user authentication information from the server device and without regard for prior authentication information in said client device; and

a remote request processing section which sets the user authentication information, included in a user authentication information setting request, in said user authentication section

when receiving said user authentication information setting request including said user authentication information from said server device over said network, and nullifies said user authentication information set in said user authentication section when receiving said nullification-of-user-authentication-information-setting request from said server device over said network.

38. The client device according to claim 37, wherein setting of said user authentication information in said user authentication section can be done only by said user authentication information setting request received from said server device.

39. The client device according to claim 37, further comprising a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received from said server device over said network.

40. The client device according to claim 37, further comprising a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again by a new user authentication information setting request received

over said network.

41. The client device according to claim 37, further comprising a use time management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user authentication information in said user authentication section.

42. The client device according to claim 41, further comprising a use time extending section which extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface.

43. The client device according to claim 37, further comprising a log-in number management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section.

44. The client device according to claim 37, further comprising an authentication nullification section which

nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface.

45-48. (canceled)

49. A client program stored in a computer readable-medium and comprising computer executable instructions for causing a computer constituting a client device to be connected to a server device over a network to function as:

a user authentication section which authenticates a user at a time of using a maintenance interface based solely on user authentication information from the server device and without regard for prior authentication information in the client device; and

a remote request processing section which sets user authentication information, included in a user authentication information setting request, in said user authentication section when receiving said user authentication information setting request including said user authentication information from said server device over said network, and nullifies said user authentication information set in said user authentication section when receiving said nullification-of-user-authentication-information-setting request from said server device over said network.

50. The client program according to claim 49, wherein setting of said user authentication information in said user authentication section can be done only by said user authentication information setting request received from said server device.

51. The client program according to claim 49, wherein said computer is further caused to function as a decryption section which decrypts encrypted user authentication information in said user authentication information setting request received from said server device over said network.

52. The client program according to claim 49, wherein said computer is further caused to function as a cutoff enforcement section which forcibly disables use of a user who is currently using said maintenance interface in case where that user authentication information which is already set in said user authentication section is set again by a new user authentication information setting request received over said network.

53. The client program according to claim 49, wherein said computer is further caused to function as a use time management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable use time has elapsed since setting of said user

authentication information in said user authentication section.

54. The client program according to claim 53, wherein said computer is further caused to function as a use time extending section which extends a remaining use time of said use time management section by a predetermined extension time only for first log-in since opening of said maintenance interface.

55. The client program according to claim 49, wherein said computer is further caused to function as a log-in number management section which nullifies said user authentication information set in said user authentication section and forcibly disables use of a user who is currently using said maintenance interface when an allowable number of log-in events has taken place since setting of said user authentication information in said user authentication section.

56. The client program according to claim 49, wherein said computer is further caused to function as an authentication nullification section which nullifies said user authentication information set in said user authentication section at a time a user of said maintenance interface ends use of said maintenance interface.

9. Evidence Appendix

None.

10. Related Proceedings Appendix

None.